DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Post Capabilities Database (PCD)

Conducted by:
Conducted by:
Bureau of Administration
Information Sharing and Services
Office of Information Programs and Services
Privacy Office
E-mail*:* **pia@state.gov**

The Department of the State
Privacy Impact Assessment for IT Projects

Introduction

The E-Government Act of 2002 (section 208) imposes new requirements on Government agencies to ensure that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain personal information.

The purpose of the new *****requirements is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Section 208 of the E-Government Act requires that agencies now conduct Privacy Impact Assessments (PIA) on all IT projects being planned, developed, implemented, and/or operating regarding individual agency information management systems. The Office of Management and Budget (OMB) has oversight of all federal agency implementation of the Privacy Act of 1974, as amended. OMB will be scrutinizing IT project budget requests based on this new requirement among those already in place. A completed PIA is also required for DOS Information Technology (IT) Security Certification and Accreditation (C&A).

The Office of Information Programs and Services is responsible for the Department-wide implementation of the Privacy Act. This Office will provide assistance in completing the assessment and will present its findings and suggestions in a report for your submission to OMB and/or other appropriate parties.

The goals accomplished in completing a PIA include:

- Providing senior DOS management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with system project managers and system owners;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and
- Providing basic documentation on the flow of personal information within DOS systems for use and review by policy and program staff, systems analysts, and security analysts.
- Going through the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place, such as secured storage media, secured transmission and access controls.

***** These requirements are drawn from the Privacy Act, Computer Security Act, the Clinger-Cohen Act, the Government Paperwork Reduction Act, the Freedom of Information Act, and Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources and A-123: Management Accountability.

Definitions

Personal Information - Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

Accuracy with respect to information that is capable of verification or susceptible of proof, within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness - all elements necessary for making a determination are present before such determination is made.

Determination - any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Necessary - a threshold of need for an element of information greater than mere relevance and utility.

Record - any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance - limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended.

Routine Use - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

System of Records - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data. (For example, tables or data arrays).

Department of State
Privacy Impact Assessment

A. CONTACT INFORMATION:

Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: pia@state.gov . If answer is yes, please complete the survey in its entirety.

YES _X__ NO___

***The following are examples of personally identifiable information:**

- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

The Department of State's (DoS), Office of Medical Services (MED), has initiated a project to develop a worldwide Post Capabilities Database (PCD). The PCD is a robust global medical information resource encompassing the availability of healthcare providers, facilities and services at the various medical posts

worldwide. The PCD shall be capable of providing medical support and logistics information for emergent and routine requirements at DoS posts worldwide.

3) What legal authority authorizes the purchase or development of this system/application?

Legal authority to procure a design and development of an electronic record system is derived from the Government Paperwork Elimination Act (GPEA), the Paperwork Reduction Act (PRA), and the e-Government Act of 2002.

C. <u>DATA IN THE SYSTEM:</u>

1) Does a Privacy Act system of records already exist?

YES ___ NO__X__

If yes, please provide the following:
System Name _____ Number ____

If no, a Privacy system of records description will need to be created for this data.

2) What categories of individuals are covered in the system?

PCD contains the names, addresses, telephone numbers and current assignments of all medical providers located in each of the 138 medical posts world-wide. Each medical provider is also identified by their medical specialty, which enables MED to arrange for regional emergent care when necessary.

3) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information in PCD pertaining to individuals is taken from each individual

b. Why is the information not being obtained directly from the individual?

Not applicable.

c. What Federal agencies are providing data for use in the system?

Not applicable.

d. What State and/or local agencies are providing data for use in the system?

Not applicable.

e. From what other third party sources will data be collected?

Not applicable.

f. What information will be collected from a State Department employee and the public?

All required information collected is from State Department employees. As mentioned above, this information includes the medical provider's name, address, post assignment and medical specialty.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The information contained in PCD is collected directly from the source.

b. How will data be checked for completeness?

MED's medical professionals use medical professional standards, which include, quality review to ensure that the information in the system is accurate.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The data in the system is current as of the last interaction/communication with the individual.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail and documented both in the system and in the system requirements document.

D. DATA CHARACTERISTICS:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Yes. The system can derive new data or create previously unavailable data about an individual through aggregation via the reporting mechanism. These reports are maintained separately in the system database.

3) Will the new data be placed in the individual's record?

No.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No.

5) How will the new data be verified for relevance and accuracy?

Not applicable.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Utilization of all PCD components used by MED and FS personnel are dependent upon access control. Access control authorizes individual module specific access rights and valid user authentification. The PCD login process is a two-tiered process. The login validates a user's security identifier (user name) and access rights/roles permissions within PCD. Within each module of PCD, each user has a specific role and permissions that apply to the function of that role within the PCD database. When a user logs on, the user's name and password are checked against the username within the Oracle database. If the username correlates to one on file, application specific access rights are granted to the user. Users are forced to change passwords every 180 days by system administrators. Users are not allowed to manually change passwords without the prompting of a system administrator.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

   See above.

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

   Data may be retrieved from the PCD using the patient's name, social security number, post assignment and medical specialty.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   PCD has the capability to deliver multiple types of reports. The reports will be used to examine trends in medical care delivery, trends in regional medical care delivery, medical conditions, and health awareness. Only Department of State medical personnel will have access to these reports based on the access control guided by their business roles.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   Not applicable.

2) **What are the retention periods of data in this system?**

   No plan currently exists for the retirement of records.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   Not applicable.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

   No.

5) **How does the use of this technology affect public/employee privacy?**

   Not applicable.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

The system will be able to identify and locate medical personnel with medical specialties when a medical emergency occurs in regions across the world. The intent of the system is to provide a mechanism for contacting medical specialists, instead of relying on MED Washington for providing emergent care.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

For monitoring purposes, the only information collected and reported are items related to any change in the capability of a medical specialist.

8) **What controls will be used to prevent unauthorized monitoring?**

Medical professional standards indicate that any unauthorized use and monitoring of medical information for reasons other than primary and emergent care is unacceptable. With that said, access to PCD and any monitoring is based on the business role of all users given access to the system.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Any changes to the system will not require a revision to the Privacy Act system of records notice, since any modifications will be within the same scope as the current system.

11) **Are there forms associated with the system? YES __X__ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Each form does contain a Privacy Act statement that includes the required information identified by the Privacy Act regulation.

F. <u>ACCESS TO DATA:</u>

1) **Who will have access to the data in the system?** (e.g., contractors, users, managers, system administrators, developers, other)

Contract and direct hire medical personnel and system administrators.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

   Access to the system and data are determined by each individual's business need and role. The access rules have been identified in the PCD User Requirements documentation.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   User access is determined by user role. If an individual's role does not require access to the system, they are restricted from accessing the system

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

   No auditing (view) functionality currently exists to determine if users needing access based on their role misuse the system and its data.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

   Contractors are involved with the design and development of the system. Each contract has Privacy Act clauses inserted thereby ensuring that the contractors are aware of their responsibilities regarding privacy. Training has been provided to all users and non-users of the system (as part of their security training) regarding the handling of information covered under the Privacy Act of 1974.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   There is currently no interface between PCD and another information based system.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Not applicable.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

   Yes, the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and select officials at the White House.

9) **If so, how will the data be used by the other agency?**

   No.

10) **Who is responsible for assuring proper use of the data?**

    Chris Cockrell, Office of Medical Services, Deputy ISSO

ADDITIONAL COMMENTS: *(optional)*

Privacy Impact Assessment Certifying Officials

System Manager

Certification _X_Yes ___No

Name: Michael Pate

Title: Medical Informatics Division Chief

IT Security Manager

Certification _X_Yes ___No

Name: Jim Thornberry

Title Operations Manager and ISSO

Privacy Coordinator

Certification _X_Yes ___No

Name: Dr. Robert Burney

The above listed certifying officials are verifying the accuracy of this document and its compliance with the Privacy Act of 1974, as amended.

Drafted: IPS/PP/LC: KFrench

Cleared: IPS/PP/LC:ASRitchie
IPS/PP:MPeppe
L/LM:JSchnitker
IPS:MGrafeld, Acting